Requested Patent: JP2002041474A

Title: AUTHENTICATION METHOD ;

Abstracted Patent: JP2002041474 ;

Publication Date: 2002-02-08 ;

Inventor(s): UNOKI TERUHIKO ;

Applicant(s): OKI ELECTRIC IND CO LTD ;

Application Number: JP20000230380 20000731 ;

Priority Number(s): ;

IPC Classification: G06F15/00; H04L9/08; H04L9/32 ;

Equivalents: ;

ABSTRACT:

PROBLEM TO BE SOLVED: To facilitate distribution, change, management, etc., of key, when authenticating, using an authenticating method by a third party organization.SOLUTION: This authenticating method, in which a server device for providing service to a client device and a key-distributing device for distributing a key used to authenticate the client device in authenticating the client device, uses a public key for encryption and a secret key for decoding and distributes a temporary use key.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－41474
(P2002－41474A)
(43)公開日　平成14年２月８日(2002.2.8)

(51)Int.Cl.⁷	識別記号	FI	テーマコード（参考）
G06F 15/00	330	G06F 15/00	330B 5B085
H04L 9/08		H04L 9/00	601A 5J104
9/32			601B
			673B
			675D

審査請求　未請求　請求項の数６　ＯＬ　（全 24 頁）

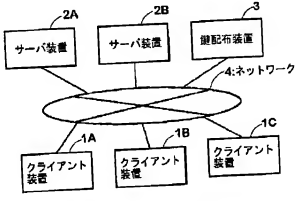
(21)出願番号　特願2000－230380(P2000－230380)
(22)出願日　平成12年７月31日(2000.7.31)

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号
(72)発明者　卯木　輝彦
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内
(74)代理人　100082050
弁理士　佐藤　幸男

Ｆターム(参考)　5B085 AE13 AE23 AE29 BE07 BG07
5J104 AA07 EA04 EA06 EA19 KA02
KA06 KA11 KA21 MA03 MA05
NA01 NA02 NA03

(54)【発明の名称】　認証方法

(57)【要約】
【課題】　第三者機関による認証方法を用いて認証するときに、鍵の配布、変更、管理等を容易にする。
【解決手段】　クライアント装置にサービスを提供するサーバ装置、及び、クライアント装置の認証に用いる鍵を配布する鍵配布装置がクライアント装置を認証する認証方法は、暗号用公開鍵及び復号用秘密鍵を用いて、一時使用鍵を配布する。



具体例１の認証システムの構成を示す図

【特許請求の範囲】
【請求項１】　クライアント装置にサービスを提供するサーバ装置、及び、前記クライアント装置の認証に用いる鍵を配布する鍵配布装置が前記クライアント装置を認証する認証方法であって、
前記鍵配布装置が前記クライアント装置を認証する第１のステップと、
前記鍵配布装置が前記クライアント装置を認証した後に、前記サーバ装置が前記クライアント装置を認証する第２のステップとを含み、
前記第１のステップは、
前記鍵配布装置が、前記鍵配布装置と前記クライアント装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を前記クライアント装置の復号用秘密鍵に対応する暗号用公開鍵で暗号化し、暗号化された一時使用鍵［ク鍵］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［ク鍵］を復号用秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、
前記クライアント装置が、前記鍵配布装置が前記クライアント装置を認証するために用いる前記クライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化された前記クライアント装置認証用データを前記鍵配布装置へ送信するステップと、
前記鍵配布装置が、暗号化された前記クライアント装置認証用データを一時使用鍵［ク鍵］で復号化することにより、前記クライアント装置認証用データを得るステップと、
前記鍵配布装置が、復号化された前記クライアント装置認証用データに基づき前記クライアント装置を認証するステップと、
前記鍵配布装置が前記クライアント装置を認証したときに、前記鍵配布装置が、前記第２のステップで前記サーバ装置が前記クライアント装置を認証するために用いる、前記クライアント装置と前記サーバ装置との間で一時的に使用可能な一時使用鍵［クサ］を前記クライアント装置及び前記サーバ装置へ送信するステップとを含むことを特徴とする認証方法。
【請求項２】　クライアント装置にサービスを提供するサーバ装置、及び、前記クライアント装置の認証に用いる鍵を配布する鍵配布装置が前記クライアント装置を認証する認証方法であって、
前記鍵配布装置が前記クライアント装置を認証する第１のステップと、
前記鍵配布装置が前記クライアント装置を認証した後に、前記サーバ装置が前記クライアント装置を認証する第２のステップとを含み、
前記第１のステップは、
前記鍵配布装置が、前記クライアント装置と前記鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を前記クライアント装置と前記鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップと、
前記クライアント装置が、前記鍵配布装置が所有する秘密鍵で暗号化された一時使用鍵［ク鍵］を前記鍵配布装置へ送信する送信ステップと、
前記鍵配布装置が、暗号化された一時使用鍵［ク鍵］を秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、
前記クライアント装置が、前記鍵配布装置が前記クライアント装置を認証するために用いる前記クライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化された前記クライアント装置認証用データを前記鍵配布装置へ送信するステップと、
前記鍵配布装置が、暗号化された前記クライアント装置認証用データを、復号化された一時使用鍵［ク鍵］で復号化することにより、前記クライアント装置認証用データを得るステップと、
前記鍵配布装置が、復号化された前記クライアント装置認証用データに基づき前記クライアント装置を認証するステップと、
前記鍵配布装置が、前記クライアント装置と前記サーバ装置との間での認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クサ］を前記クライアント装置へ送信するステップとを含み、
前記鍵配布装置が前記クライアント装置へ一時使用鍵［クサ］を送信するステップは、
前記鍵配布装置が前記クライアント装置へ、次回の前記送信ステップで前記クライアント装置が前記鍵配布装置へ送信すべき、秘密鍵で暗号化された一時使用鍵［ク鍵］を送信するステップを有することを特徴とする認証方法。
【請求項３】　クライアント装置、前記クライアント装置にサービスを提供するサーバ装置、及び、認証に用いる鍵を配布する鍵配布装置の間で互いに認証する認証方法であって、
前記鍵配布装置が前記クライアント装置を認証する第１のステップと、
前記鍵配布装置が前記クライアント装置を認証した後に、前記サーバ装置が前記クライアント装置を認証する第２のステップと、
前記サーバ装置が前記クライアント装置を認証した後に、前記クライアント装置が前記サーバ装置を認証する第３のステップとを含み、

前記第１のステップは、
前記鍵配布装置が、前記クライアント装置と前記鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を前記クライアント装置と前記鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップとを有し、
前記第２のステップは、
前記鍵配布装置が、前記クライアント装置と前記サーバ装置との間で認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クサ］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［クサ］を一時使用鍵［ク鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、
前記クライアント装置が、前記鍵配布装置と前記サーバ装置との間の共通鍵［サ鍵］で暗号化された一時使用鍵［クサ］を前記サーバ装置へ送信する送信ステップと、
前記サーバ装置が、暗号化された一時使用鍵［クサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、
前記クライアント装置が、前記クライアント装置を認証するための前記クライアント装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化された前記クライアント装置認証用データを前記サーバ装置へ送信するステップと、
前記サーバ装置が、暗号化された前記クライアント装置認証用データを、一時使用鍵［クサ］で復号化することにより、前記クライアント装置認証用データを得るステップと、
前記サーバ装置が、前記クライアント装置認証用データに基づき前記クライアント装置を認証するステップとを有し、
前記第３のステップは、
前記サーバ装置が、前記サーバ装置を認証するための前記サーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化された前記サーバ装置認証用データを前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された前記サーバ装置認証用データを一時使用鍵［クサ］で復号化することにより、前記サーバ装置認証用データを得るステップと、
前記クライアント装置が、前記サーバ装置認証用データに基づき前記サーバ装置を認証するステップとを有し、
前記サーバ装置が前記クライアント装置に前記サーバ装置認証用データを送信するステップは、前記サーバ装置が前記クライアント装置に、次回の送信ステップで前記クライアント装置が前記サーバ装置へ送信すべき、共通鍵［サ鍵］で暗号化された一時使用鍵［クサ］を送信するステップを有することを特徴とする認証方法。

【請求項４】　ネットワークを介してクライアント装置にサービスを提供するサーバ装置、及び、リンクを介して前記サーバ装置に接続されており認証に用いる鍵をネットワーク及びリンクを介して配布する鍵配布装置が前記クライアント装置を認証する認証方法であって、
前記鍵配布装置が前記クライアント装置を認証する第１のステップと、
前記鍵配布装置が前記クライアント装置を認証した後に、前記サーバ装置が前記クライアント装置を認証する第２のステップとを含み、前記第１のステップは、
前記鍵配布装置が、前記クライアント装置と前記鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を前記クライアント装置と前記鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップと、
前記第２のステップは、
前記クライアント装置が、前記サーバ装置が前記クライアント装置を認証するために用いる前記クライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化された前記クライアント装置認証用データを前記鍵配布装置へ送信するステップと、
前記鍵配布装置が、暗号化された前記クライアント装置認証用データを一時使用鍵［ク鍵］で復号化することにより、前記クライアント装置認証用データを得るステップと、
前記鍵配布装置が、前記クライアント装置認証用データを共通鍵［サ鍵］で暗号化し、暗号化された前記クライアント装置認証用データを前記サーバ装置へ送信するステップと、
前記サーバ装置が、暗号化された前記クライアント装置認証用データを共通鍵［サ鍵］で復号化することにより、前記クライアント装置認証用データを得るステップと、
前記サーバ装置が、前記クライアント装置認証用データに基づき前記クライアント装置を認証するステップとを含むことを特徴とする認証方法。

【請求項５】　エージェント装置が、クライアント装置にサービスを提供するサーバ装置、及び前記クライアント装置の認証に用いる鍵を配布する鍵配布装置と、前記クライアント装置との間での認証を代行するする認証方法であって、
前記エージェント装置が、前記クライアント装置を認証する第１のステップと、

前記エージェント装置が前記クライアント装置を認証した後に、前記サーバ装置が、前記エージェント装置を認証する第2のステップとを含み、

前記第1のステップは、

前記鍵配布装置が、前記クライアント装置と前記エージェント装置との間での認証のために一時的に使用可能な一時使用鍵［クエ］を前記クライアント装置と前記鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クエ］を前記クライアント装置へ送信するステップと、

前記クライアント装置が、暗号化された一時使用鍵［クエ］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［クエ］を得るステップと、

前記鍵配布装置が、一時使用鍵［クエ］を前記エージェント装置と前記鍵配布装置との間の共通鍵［エ鍵］で暗号化し、暗号化された一時使用鍵［クエ］を前記エージェント装置へ送信するステップと、

前記エージェント装置が、暗号化された一時使用鍵［クエ］を共通鍵［エ鍵］で復号化することにより、一時使用鍵［クエ］を得るステップと、

前記クライアント装置が、前記エージェント装置が前記クライアント装置を認証するために用いる前記クライアント装置認証用データを一時使用鍵［クエ］で暗号化し、暗号化された前記クライアント装置認証用データを前記エージェント装置へ送信するステップと、

前記エージェント装置が、暗号化された前記クライアント装置認証用データを一時使用鍵［クエ］で復号化することにより、前記クライアント装置認証用データを得るステップと、

前記エージェント装置が、前記クライアント装置認証用データに基づき前記クライアント装置を認証するステップと、

前記第2のステップは、

前記鍵配布装置が、前記エージェント装置と前記サーバ装置との間での認証のために一時的に使用可能な一時使用鍵［エサ］を前記鍵配布装置と前記エージェント装置との間の共通鍵［エ鍵］で暗号化し、暗号化された一時使用鍵［エサ］を前記エージェント装置へ送信するステップと、

前記エージェント装置が、暗号化された一時使用鍵［エサ］を共通鍵［エ鍵］で復号化することにより、一時使用鍵［エサ］を得るステップと、

前記鍵配布装置が、一時使用鍵［エサ］を前記鍵配布装置と前記サーバ装置との間の共通鍵［サ鍵］で暗号化し、暗号化された一時使用鍵［エサ］を前記サーバ装置へ送信するステップと、

前記サーバ装置が、暗号化された一時使用鍵［エサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［エサ］を得るステップと、

前記エージェント装置が、前記サーバ装置が前記エージェント装置を認証するために用いる前記エージェント装置認証用データを一時使用鍵［エサ］で暗号化し、暗号化された前記エージェント装置認証用データを前記サーバ装置へ送信するステップと、

前記サーバ装置が、暗号化された前記エージェント装置認証用データを一時使用鍵［エサ］で復号化することにより、前記エージェント装置認証用データを得るステップと、

前記サーバ装置が、前記エージェント装置認証用データに基づき前記エージェント装置を認証するステップとを含むことを特徴とする認証方法。

【請求項6】　クライアント装置が、前記クライアント装置にサービスを提供するサーバ装置、及び、認証に用いる鍵を配布する鍵配布装置を認証する認証方法であって、

前記クライアント装置が前記鍵配布装置を認証する第1のステップと、

前記クライアント装置が前記鍵配布装置を認証した後に、前記クライアント装置が前記サーバ装置を認証する第2のステップとを含み、

前記第1のステップは、

前記クライアント装置が、前記クライアント装置と前記鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を前記鍵配布装置の復号用秘密鍵に対応する暗号用公開鍵で暗号化し、暗号化された一時使用鍵［ク鍵］を前記鍵配布装置へ送信するステップと、

前記鍵配布装置が、暗号化された一時使用鍵［ク鍵］を復号用秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、

前記クライアント装置が、前記クライアント装置が前記鍵配布装置を認証するために用いる前記鍵配布装置認証用データを暗号用公開鍵で暗号化し、暗号化された前記鍵配布装置認証用データを前記鍵配布装置へ送信するステップと、

前記鍵配布装置が、暗号化された前記鍵配布装置認証用データを復号用秘密鍵で復号化することにより、前記鍵配布装置認証用データを得るステップと、

前記鍵配布装置が、前記鍵配布装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化された前記鍵配布装置認証用データを前記クライアント装置へ送信するステップと、

前記クライアント装置が、暗号化された前記鍵配布装置認証用データを一時使用鍵［ク鍵］で復号化することにより、前記鍵配布装置認証用データを得るステップと、

前記クライアント装置が、前記鍵配布装置認証用データに基づき前記鍵配布装置を認証するステップとを有し、

前記第2のステップは、

前記鍵配布装置が、前記クライアント装置と前記サーバ装置との間での認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［ク鍵］で暗号化し、暗号化

された一時使用鍵［クサ］を前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された一時使用鍵［クサ］を一時使用鍵［クk鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、
前記鍵配布装置が、一時使用鍵［クサ］を前記鍵配布装置と前記サーバ装置との間の共通鍵［サ鍵］で暗号化し、暗号化された一時使用鍵［クサ］を前記サーバ装置へ送信するステップと、
前記サーバ装置が、暗号化された一時使用鍵［クサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、
前記クライアント装置が、前記クライアント装置が前記サーバ装置を認証するために用いる前記サーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化された前記サーバ装置認証用データを前記サーバ装置へ送信するステップと、
前記サーバ装置が、暗号化された前記サーバ装置認証用データを一時使用鍵［クサ］で復号化することにより、前記サーバ装置認証用データを得るステップと、
前記サーバ装置が、前記サーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化された前記サーバ装置認証用データを前記クライアント装置へ送信するステップと、
前記クライアント装置が、暗号化された前記サーバ装置認証用データを一時使用鍵［クサ］で復号化することにより、前記サーバ装置認証用データを得るステップと、
前記クライアント装置が、前記サーバ装置認証用データに基づき前記サーバ装置を認証するステップとを含むことを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、分散処理システムに用いられる認証方法に関する。

【0002】

【従来の技術】分散された資源をサービスとしてネットワーク経由でサーバ装置からクライアント装置へ提供する分散処理システムでは、資源は、ネットワーク上で、盗聴、改竄、偽造等から守られる必要がある。そのために、サーバ装置とクライアント装置との間で認証が行われる。認証方法として、信頼できる第三者機関が配布する認証用鍵を用いる方法がある。以下、この第三者機関を鍵配布装置という。

【0003】第三者機関による認証方法によれば、鍵配布装置によって配布される、特定の装置同士の間で一時的に使用可能な一時使用鍵を用いて認証が行われる。具体的には、まず、クライアント装置と鍵配布装置との間での一時使用鍵（以下、「一時使用鍵［ク鍵］」という。）を用いて、両装置間の認証を行い、次に、クライアント装置とサーバ装置との間での一時使用鍵（以下、「一時使用鍵［クサ］」という。）を用いて両装置間の認証を行う。

【0004】前者の認証は、クライアント装置及び鍵配布装置が、共通鍵暗号化方式に従う共通鍵（以下、共通鍵［ク鍵］という。）を予め所有していることを前提とする。この前提の下に、鍵配布装置は、共通鍵［ク鍵］を用いて暗号化された一時使用鍵［ク鍵］をクライアント装置に配布し、クライアント装置は、その暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］を用いて復号化することにより、元の一時使用鍵［ク鍵］を得る。クライアント装置が一時使用鍵［ク鍵］を得ると、両装置は、両装置間の認証のために用いる認証用データに、一時使用鍵［ク鍵］を用いて暗号化や復号化を施すことにより交換し、この認証用データに基づき認証を行う。

【0005】後者の認証は、鍵配布装置とサーバ装置が、共通鍵暗号化方式に従う共通鍵（以下、共通鍵［サ鍵］という。）を予め所有していることを前提とする。この前提の下に、鍵配布装置は、一時使用鍵［ク鍵］を用いて暗号化された一時使用鍵［クサ］をクライアント装置に配布し、また、共通鍵［サ鍵］を用いて暗号化された一時使用鍵［クサ］をクライアント装置を介してサーバ装置に配布する。クライアント装置は、暗号化された一時使用鍵［クサ］を一時使用鍵［ク鍵］を用いて復号化することにより元の一時使用鍵［クサ］を得て、また、サーバ装置は、暗号化された一時使用鍵［クサ］を共通鍵［サ鍵］を用いて復号化することにより元の一時使用鍵［クサ］を得る。両装置が一時使用鍵［クサ］を得ると、両装置は、両装置間の認証のために用いる認証用データに、一時使用鍵［クサ］を用いて暗号化や復号化を施すことにより交換し、この認証用データに基づき認証を行う。

【0006】

【発明が解決しようとする課題】しかしながら、このような第三者機関によって配布される鍵を用いる認証方法には、次のように数々の問題がある。第一に、一時使用鍵［ク鍵］を配布するために共通鍵［ク鍵］を用いることから、鍵配布装置は、ネットワーク上で共通鍵［ク鍵］自身が盗聴されることを回避すべく、共通鍵［ク鍵］をネットワーク以外の経路、例えば、手渡し、郵送、又は専用回線によりクライアント装置に配布する必要がある。また、共通鍵［ク鍵］が長時間にわたる試行錯誤の繰り返しにより、即ち総当たりにより解読されることを回避すべく、共通鍵［ク鍵］を定期的に変更することが必要になる。さらに、共通鍵［ク鍵］はクライアント装置毎に異ならなければならないことから、クライアント装置の数と同数の共通鍵［ク鍵］を管理しなければならない。

【0007】第二に、一時使用鍵［ク鍵］や一時使用鍵［クサ］のような一時使用鍵は、一定の期間内であれば利用者を問わず有効であることから、一時使用鍵を入手

した第三者が、その期間内に一時使用鍵をそのまま再利用するという、いわゆるリプレイ攻撃をすることができるおそれがある。また、第三者が、一時使用鍵を用いて総当たりの試みを行うことにより、共通鍵［ク鍵］や共通鍵［サ鍵］を解読するおそれがある。

【0008】第三に、鍵配布装置は、一時使用鍵［クサ］をクライアント装置経由でサーバ装置に配布することから、ネットワークのトラフィックが増大する。

【0009】第四に、クライアント装置は、自己を鍵配布装置やサーバ装置によって認証されることなく資源を享受することや、クライアント装置が鍵配布装置やサーバ装置を一方的に認証するだけで資源を享受することを希望しても、そのような享受は、クライアント装置を必ず認証する従来の認証方法では不可能である。

【0010】

【課題を解決するための手段】上記の問題を解決するために、本発明の第１の認証方法によれば、クライアント装置にサービスを提供するサーバ装置、及び、クライアント装置の認証に用いる鍵を配布する鍵配布装置がクライアント装置を認証する認証方法であって、鍵配布装置がクライアント装置を認証する第１のステップと、鍵配布装置がクライアント装置を認証した後に、サーバ装置がクライアント装置を認証する第２のステップとを含み、第１のステップは、鍵配布装置が、鍵配布装置とクライアント装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］をクライアント装置の復号用秘密鍵に対応する暗号用公開鍵で暗号化し、暗号化された一時使用鍵［ク鍵］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［ク鍵］を復号用秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、クライアント装置が、鍵配布装置がクライアント装置を認証するために用いるクライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化されたクライアント装置認証用データを鍵配布装置へ送信するステップと、鍵配布装置が、暗号化されたクライアント装置認証用データを一時使用鍵［ク鍵］で復号化することにより、クライアント装置認証用データを得るステップと、鍵配布装置が、復号化されたクライアント装置認証用データに基づきクライアント装置を認証するステップと、鍵配布装置がクライアント装置を認証したときに、鍵配布装置が、第２のステップでサーバ装置がクライアント装置を認証するために用いる、クライアント装置とサーバ装置との間で一時的に使用可能な一時使用鍵［クサ］をクライアント装置及びサーバ装置へ送信するステップとを含む。

【0011】本発明の第２の認証方法によれば、クライアント装置にサービスを提供するサーバ装置、及び、クライアント装置の認証に用いる鍵を配布する鍵配布装置がクライアント装置を認証する認証方法は、鍵配布装置がクライアント装置を認証する第１のステップと、鍵配布装置がクライアント装置を認証した後に、サーバ装置がクライアント装置を認証する第２のステップとを含み、第１のステップは、鍵配布装置が、クライアント装置と鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］をクライアント装置と鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップと、クライアント装置が、鍵配布装置が所有する秘密鍵で暗号化された一時使用鍵［ク鍵］を鍵配布装置へ送信する送信ステップと、鍵配布装置が、暗号化された一時使用鍵［ク鍵］を秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、クライアント装置が、鍵配布装置がクライアント装置を認証するために用いるクライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化されたクライアント装置認証用データを鍵配布装置へ送信するステップと、鍵配布装置が、暗号化されたクライアント装置認証用データを、復号化された一時使用鍵［ク鍵］で復号化することにより、クライアント装置認証用データを得るステップと、鍵配布装置が、復号化されたクライアント装置認証用データに基づきクライアント装置を認証するステップと、鍵配布装置が、クライアント装置とサーバ装置との間での認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クサ］をクライアント装置へ送信するステップとを含み、鍵配布装置がクライアント装置へ一時使用鍵［クサ］を送信するステップは、鍵配布装置がクライアント装置へ、次回の送信ステップでクライアント装置が鍵配布装置へ送信すべき、秘密鍵で暗号化された一時使用鍵［ク鍵］を送信するステップを有する。

【0012】本発明の第３の認証方法によれば、クライアント装置、クライアント装置にサービスを提供するサーバ装置、及び、認証に用いる鍵を配布する鍵配布装置の間で互いに認証する認証方法は、鍵配布装置がクライアント装置を認証する第１のステップと、鍵配布装置がクライアント装置を認証した後に、サーバ装置がクライアント装置を認証する第２のステップと、サーバ装置がクライアント装置を認証した後に、クライアント装置がサーバ装置を認証する第３のステップとを含み、第１のステップは、鍵配布装置が、クライアント装置と鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］をクライアント装置と鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップとを有し、第２のステップは、

鍵配布装置が、クライアント装置とサーバ装置との間で認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［クタ］で暗号化し、暗号化された一時使用鍵［クサ］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［クサ］を一時使用鍵［クタ］で復号化することにより、一時使用鍵［クサ］を得るステップと、クライアント装置が、鍵配布装置とサーバ装置との間の共通鍵［サ鍵］で暗号化された一時使用鍵［クサ］をサーバ装置へ送信する送信ステップと、サーバ装置が、暗号化された一時使用鍵［クサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、クライアント装置が、クライアント装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化されたクライアント装置認証用データをサーバ装置へ送信するステップと、サーバ装置が、暗号化されたクライアント装置認証用データを、一時使用鍵［クサ］で復号化することにより、クライアント装置認証用データを得るステップと、サーバ装置が、クライアント装置認証用データに基づきクライアント装置を認証するステップとを有し、第3のステップは、サーバ装置が、サーバ装置を認証するためのサーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化されたサーバ装置認証用データをクライアント装置へ送信するステップと、クライアント装置が、暗号化されたサーバ装置認証用データを一時使用鍵［クタ］で復号化することにより、サーバ装置認証用データを得るステップと、クライアント装置が、サーバ装置認証用データに基づきサーバ装置を認証するステップとを有し、サーバ装置がクライアント装置にサーバ装置認証用データを送信するステップは、サーバ装置がクライアント装置に、次回の送信ステップでクライアント装置がサーバ装置へ送信すべき、共通鍵［サ鍵］で暗号化された一時使用鍵［クサ］を送信するステップを有する。

【0013】本発明の第4の認証方法によれば、ネットワークを介してクライアント装置にサービスを提供するサーバ装置、及び、リンクを介してサーバ装置に接続されており認証に用いる鍵をネットワーク及びリンクを介して配布する鍵配布装置がクライアント装置を認証する認証方法は、鍵配布装置がクライアント装置を認証する第1のステップと、鍵配布装置がクライアント装置を認証した後に、サーバ装置がクライアント装置を認証する第2のステップとを含み、第1のステップは、鍵配布装置が、クライアント装置と鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］をクライアント装置と鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［ク鍵］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［ク鍵］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［ク鍵］を得るステップと、第2のステップは、クライアント装置が、サーバ装置がクライアント装置を認証するために用いるクライアント装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化されたクライアント装置認証用データを鍵配布装置へ送信するステップと、鍵配布装置が、暗号化されたクライアント装置認証用データを一時使用鍵［ク鍵］で復号化することにより、クライアント装置認証用データを得るステップと、鍵配布装置が、クライアント装置認証用データを共通鍵［サ鍵］で暗号化し、暗号化されたクライアント装置認証用データをサーバ装置へ送信するステップと、サーバ装置が、暗号化されたクライアント装置認証用データを共通鍵［サ鍵］で復号化することにより、クライアント装置認証用データを得るステップと、サーバ装置が、クライアント装置認証用データに基づきクライアント装置を認証するステップとを含む。

【0014】本発明の第5の認証方法によれば、エージェントが、クライアント装置にサービスを提供するサーバ装置、及びクライアント装置の認証に用いる鍵を配布する鍵配布装置と、クライアント装置との間での認証を代行するする認証方法は、エージェントが、クライアント装置を認証する第1のステップと、エージェントがクライアント装置を認証した後に、サーバ装置が、エージェントを認証する第2のステップとを含み、第1のステップは、鍵配布装置が、クライアント装置とエージェントとの間での認証のために一時的に使用可能な一時使用鍵［クエ］をクライアント装置と鍵配布装置との間の共通鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クエ］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［クエ］を共通鍵［ク鍵］で復号化することにより、一時使用鍵［クエ］を得るステップと、鍵配布装置が、一時使用鍵［クエ］をエージェントと鍵配布装置との間の共通鍵［エ鍵］で暗号化し、暗号化された一時使用鍵［クエ］をエージェントへ送信するステップと、エージェントが、暗号化された一時使用鍵［クエ］を共通鍵［エ鍵］で復号化することにより、一時使用鍵［クエ］を得るステップと、クライアント装置が、エージェントがクライアント装置を認証するために用いるクライアント装置認証用データを一時使用鍵［クエ］で暗号化し、暗号化されたクライアント装置認証用データをエージェントへ送信するステップと、エージェントが、暗号化されたクライアント装置認証用データを共通鍵［サ鍵］で復号化することにより、クライアント装置認証用データを得るステップと、エージェントが、クライアント装置認証用データに基づきクライアント装置を認証するステップと、第2のステップは、鍵配布装置が、エージェントとサーバ装置との間での認証のために一時的に使用可能な一時使用鍵［エサ］を鍵配布装置とエージェントとの間の共通鍵［エ鍵］で暗号化し、暗号化された一時使用鍵［エ

サ]をエージェントへ送信するステップと、エージェントが、暗号化された一時使用鍵［エサ］を共通鍵［エ鍵］で復号化することにより、一時使用鍵［エサ］を得るステップと、鍵配布装置が、一時使用鍵［エサ］を鍵配布装置とサーバ装置との間の共通鍵［サ鍵］で暗号化し、暗号化された一時使用鍵［エサ］をサーバ装置へ送信するステップと、サーバ装置が、暗号化された一時使用鍵［エサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［エサ］を得るステップと、エージェントが、サーバ装置がエージェントを認証するために用いるエージェント認証用データを一時使用鍵［エサ］で暗号化し、暗号化されたエージェント認証用データをサーバ装置へ送信するステップと、サーバ装置が、暗号化されたエージェント認証用データを一時使用鍵［エサ］で復号化することにより、エージェント認証用データを得るステップと、サーバ装置が、エージェント認証用データに基づきエージェントを認証するステップとを含む。

【００１５】本発明の第６の認証方法によれば、クライアント装置が、クライアント装置にサービスを提供するサーバ装置、及び、認証に用いる鍵を配布する鍵配布装置を認証する認証方法であって、クライアント装置が鍵配布装置を認証する第１のステップと、クライアント装置が鍵配布装置を認証した後に、クライアント装置がサーバ装置を認証する第２のステップとを含み、第１のステップは、クライアント装置が、クライアント装置と鍵配布装置との間での認証のために一時的に使用可能な一時使用鍵［ク鍵］を鍵配布装置の復号用秘密鍵に対応する暗号用公開鍵で暗号化し、暗号化された一時使用鍵［ク鍵］を鍵配布装置へ送信するステップと、鍵配布装置が、暗号化された一時使用鍵［ク鍵］を鍵配布装置の復号用秘密鍵で復号化することにより、一時使用鍵［ク鍵］を得るステップと、クライアント装置が、クライアント装置が鍵配布装置を認証するために用いる鍵配布装置認証用データを暗号用公開鍵で暗号化し、暗号化された鍵配布装置認証用データを鍵配布装置へ送信するステップと、鍵配布装置が、暗号化された鍵配布装置認証用データを復号用秘密鍵で復号化することにより、鍵配布装置認証用データを得るステップと、鍵配布装置が、鍵配布装置認証用データを一時使用鍵［ク鍵］で暗号化し、暗号化された鍵配布装置認証用データをクライアント装置へ送信するステップと、クライアント装置が、暗号化された鍵配布装置認証用データを一時使用鍵［ク鍵］で復号化することにより、鍵配布装置認証用データを得るステップと、クライアント装置が、鍵配布装置認証用データに基づき鍵配布装置を認証するステップとを有し、第２のステップは、鍵配布装置が、クライアント装置とサーバ装置との間での認証のために一時的に使用可能な一時使用鍵［クサ］を一時使用鍵［ク鍵］で暗号化し、暗号化された一時使用鍵［クサ］をクライアント装置へ送信するステップと、クライアント装置が、暗号化された一時使用鍵［クサ］を一時使用鍵［ク鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、鍵配布装置が、一時使用鍵［クサ］を鍵配布装置とサーバ装置との間の共通鍵［サ鍵］で暗号化し、暗号化された一時使用鍵［クサ］をサーバ装置へ送信するステップと、サーバ装置が、暗号化された一時使用鍵［クサ］を共通鍵［サ鍵］で復号化することにより、一時使用鍵［クサ］を得るステップと、クライアント装置が、クライアント装置がサーバ装置を認証するために用いるサーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化されたサーバ装置認証用データをサーバ装置へ送信するステップと、サーバ装置が、暗号化されたサーバ装置認証用データを一時使用鍵［クサ］で復号化することにより、サーバ装置認証用データを得るステップと、サーバ装置が、サーバ装置認証用データを一時使用鍵［クサ］で暗号化し、暗号化されたサーバ装置認証用データをクライアント装置へ送信するステップと、クライアント装置が、暗号化されたサーバ装置認証用データを一時使用鍵［クサ］で復号化することにより、サーバ装置認証用データを得るステップと、クライアント装置が、サーバ装置認証用データに基づきサーバ装置を認証するステップとを含む。

【００１６】

【発明の実施の形態】以下、発明の実施の形態について説明する。実施の形態として、具体例１～具体例６を説明する。具体例１は、クライアント装置と鍵配布装置との間の鍵として暗号用公開鍵及び復号用秘密鍵を用いることを主な特徴とする。具体例２及び具体例３は、鍵配布装置がクライアント装置へ次回使用すべきチケット交付チケットＴＧＴまたはサービスチケットＳＴを送信することを主な特徴とする。具体例４は、鍵配布装置がサーバ装置へサービスチケットＳＴを直接配布することを特徴とする。具体例５は、エージェント装置６がクライアント装置、鍵配布装置、及びサーバ装置の間で行うべき手続の一部を代行することを主な特徴とする。具体例６は、クライアント装置が鍵配布装置またはサーバ装置によって認証されることなくサービスを提供されることを主な特徴とする。

【００１７】〈具体例１〉図１は、具体例１の認証システムの構成を示す図である。図示されるように、認証システムは、複数のクライアント装置１Ａ～１Ｃ、複数のサーバ装置２Ａ、２Ｂ、鍵配布装置３、及び、ネットワーク４を含む。これらの装置１、２、３は、ネットワーク４を介して、認証やサービスの授受のために、装置の識別番号、装置を認証するための認証用データ、暗号化／復号化のための鍵等を含む暗号化されたメッセージ（以下、［暗号化メッセージ］という。）やチケット等を交換する。ここで、チケットとは、暗号化メッセージのうち、サービスの提供や享受に関するものをいう。

【００１８】クライアント装置１Ａ～１Ｃは、例えば、